The Year 2000 Crisis

By: Tom Mooney

Tyler Fire Department

Tyler, Texas

An applied research project submitted to the National Fire Academy as part of the

Executive Fire Officer Program

April 1998

ABSTRACT

The Year 2000 Crisis will challenge a computer technology dependent world. Many computer systems rely on a year representation of the last two-digits of the year. The year 2000 would be represented as "00" and may be misinterpreted as the year 1900 instead. The ambiguity may affect all date sensitive transactions and cause problems ranging from bad data to system failures. Thus the Year 2000 Crisis is born.

The purpose of the research was to evaluate the Year 2000 Crisis, the impact it may have on the fire service, and methods of mitigation. The full impact of the crisis is not fully understood. However, the consequences of doing nothing about the problem may prove reckless and irresponsible. Research revealed a high probability of a crisis materializing as the year 2000 draws near.

The author used an evaluative approach to answer the following research questions:

1.) What is the Year 2000 Crisis?

2.) What will be the impact of the Year 2000 Crisis?

3.) To what extent does the fire service depend on computer technology?

4.) What steps can be taken to mitigate the Year 2000 Crisis?

A research project was selected based on the need for strategic planning. The Year 2000 Crisis was determined to be of significant concern and probable impact in the future as to warrant serious research. Literature review was conducted and interviews of technology professionals were conducted. A survey was also administered to fire service colleagues.

The research results indicate the Year 2000 Crisis to be of a grave concern and impact as to warrant immediate attention. The inability of computer technology to function properly would have an adverse affect on mission critical services.

Strategic planning will be required to mitigate the developing crisis. The author recommends mitigation efforts to begin and include:

1. Computer technology inventory.
2. Assess Year 2000 risk of inventory.
3. Contact vendors. Plan and repair suspect inventory.
4. Implement upgrade.
5. Test upgrade for Year 2000 compliance.

TABLE OF CONTENTS

INTRODUCTION

What could possibly be the most extensive and costly computer maintenance project the world has ever seen is known as the Year 2000 Crisis. Many computer systems today rely on a year representation of only the last two digits of the year. The year 1998 is usually stored as "98". As a result, the year 2000 is represented as "00" and is interpreted as the year 1900 instead of the year 2000. The ambiguity affects all date sensitive transactions. Problems can result from misinterpreting the year digits that range from bad data to system failures as maintenance schedules, contracts, and other time sensitive data are seen as 100 years old. The consequences of such a wrong date interpretation can be serious.

The purpose of this research is to evaluate the Year 2000 Crisis, it's impact, and the process involved in mitigating the problem. To the extent the Year 2000 Crisis will impact the fire service is not known. However, it appears reasonable to examine the issue due to the possible negative impact the year 2000, sometimes abbreviated as Y2K, may have on the fire service. Can the administrative functions or more importantly, the fire emergency services be disrupted as a result of a failure in a computer or microprocessor? If so, what steps might the fire service take to mitigate the impact of any Y2K problem?

This author used the evaluative research method for this project. The author examines the Year 2000 issue, the extent of the problem, fire department use of computer technology, and Year 2000 Crisis mitigation. The impact of the Year 2000 Crisis is directly related to technological dependency on computers and equipment that is computerized or has microprocessors. If a crisis is pending, what steps can be taken to mitigate the Y2K threat?

The research questions are:

1. What is the Year 2000 Crisis?
2. What will be the impact of the Year 2000 Crisis?
3. To what extent does the fire service depend on computer technology?
4. What steps can be taken to mitigate the Year 2000 Crisis?

BACKGROUND AND SIGNIFINANCE

Computers have not always been small. There was a time, in the development of the computer, when computers were large – even room size. However, being large did not imply large amounts of room for data. As a matter of fact, data capacity was very limited. For this reason, programmers were forced to conserve internal memory and disc space. Shortening the year representation on all date related data from four to two digits saved capacity. For each date represented by two digits instead of four digits, programmers saved two bytes of information per occurrence. This translated to tremendous savings in memory space. As computers improved, the capacity limitations became less critical and was no longer a major factor. However, in the 1990's as space limitations were a minor issue, programmers still utilized a two-digit year representation instead of going o a four-digit representation. No one seem to consider that the year 2000 and how the representation of that year as "00" would impact computer programming. As a computer reads "00", the year may be interpreted as 1900 instead of 2000 because of the programming. This misinterpretation may result in a miscalculation or malfunction of the computer system.

The impact of the Year 2000 Crisis affects two broad categories: Software and Hardware. The software includes the internally developed applications, vendor applications, office automation, word processing, desktop publication, and other operating systems. E-mail, voice mail, scheduling systems and other back-up systems are also impacted by the date data interpretations. The hardware impacted is computers, printers, routers, and other peripherals. Some other systems include hardware in ATM bank machine, copiers, fax machines, elevators, and security systems. Some climate control systems are affected as well. Bank vaults, lighting systems, phone switchboards, traffic control systems and satellite systems are also impacted.

According to industry experts, it will cost approximately $600 billion worldwide to fix the problems associated with the Year 2000 Crisis. Such an expensive and extensive issue worldwide will impact almost everyone including those in the fire service. There are internal and external impact considerations for the fire service as computer technology is used throughout the environment in which it operates.

The Year 2000 Crisis is an impending disaster. It is not unlike planning for other disasters in the emergency management sector. The analytical and mitigation characteristics of the fire service in addressing impending disasters will be mandatory. The Executive Planning course in the Executive Fire Officer's Program lends itself to such an important pre-planning effort.

LITERATURE REVIEW

Year 2000 crisis overview

The Year 2000 Crisis, Y2K, or the Millennium Bug as it is sometimes referred to, is getting more and more attention. It is seen as one of the most important challenges to businesses and government ever. Although awareness of the problem is growing, many have an imperfect comprehension of the issues related to the Y2K problem. "Effective resolution begins with an understanding of the nature of the Y2K problem, how it originated, and the implications involved." (Granger, p.2) The millennium bug results from the common six-digit date representation used in computer programs. To save space, programmers abbreviated the four-digit representation of a year to a two-digit representation using the last two digits. A typical program would represent the year 1998 simply as "98". The problem with the representation is that it assumes that all activities will occur in the same century. The results of a date calculation in the twenty-first century would produce a wrong answer. For example, if a program needs to calculate a person's age, the program would subtract the current year from the year of the person's birth. If the person was born in 1960 and if it is now 1998, the computer would calculate the age to be 38 by subtracting 60 from 98. But if the current year were 2000, the computer would calculate the age by subtracting 60 from 00, resulting in an age of –60 years of age. The computer may recognize a negative number for the age to be in error and would not go any further or it may make an error using the age. In either case, the program would not work as intended (Grange and Helms, 1998).

The problem started more than thirty years ago during the infancy of computer technology. When designing computer applications, computer programmers limited the number of available spaces for representing the date in order to conserve space. The internal memory was very limited and expensive.

The format for dates was MM/DD/YY, which limited the year to two digits in each date data field. This works well until the year 2000 arrives. Then the computer does not see "00" as the year 2000 but as 1900 and will miscalculate all related computations (Muhammad, 1997).

Simons (1997) estimates that on January 1, 2000, some 90% of the world's computer hardware and software will "think" it is the first day of 1900. "What sounds like a simple computer glitch will have enormous business ramifications." (Simons, p. 54) Although the majority of problems will occur in the year 2000, there will be problems occurring earlier as computers process information which extends past the, now near, date of 2000 (Simons, 1997).

Virtually every government, state, municipality and business in the world is going to have to have to deal with the Year 2000 problem. In fact, if they haven't started already it may be too late because fixing the problem can take a lot of time and will be expensive. The bill for all of the work that has to be done to address the problem could go as high as $600 billion (Levy and Hafner, 1997).

Accounting properties, tax technicalities and finding funding will take a toll on the Year 2000 problem solving. The Financial Accounting and Standards Board has ruled that internal and external costs associated with modifying computer software for the Year 2000 must be charged to all businesses as incurred. This would mean that companies choosing to repair their software couldn't amortize the costs over several years. However, the ruling does not address the purchase of software replacing those not in Year 2000 compliance (Simonelli, 1997).

Year 2000 compliance is one of those terms that few have a full technical understanding of what it really is. When the term "year 2000 compliant" is used, the common understanding is that issues regarding the year 2000 are resolved. However, a formal definition of compliance really means a standard is required to measure when, and how, a year 2000 conversion effort is complete and

accurate. The definition must cover three areas of integrity: 1.) General integrity, 2.) Date integrity and 3.) Century integrity. Chaabouni (1998) says the general integrity of a system is not impaired or will otherwise produce erroneous information as a result of processing current date data. He goes on to explain that date integrity will allow all manipulations of date data within a system. Century integrity refers to either four digit or two digit year applications across a century field (Chaabouni, 1998).

In order to assess the overall risks of the Year 2000 problem, it is important to realize the immense grip that information technology holds on the world. Companies are evolving into a highly intertwined mix of technology and people where one becomes inseparable from the other. Many business processes are linked to the information systems and the failure of this technological infrastructure will have an irreparable impact on critical business functions. The interconnectivity of these systems with other external systems involves the sharing of data that is passed among them which may or may not be Year 2000 compliant. Many systems creating or updating databases or files are unaware of other systems that use data at another time and in another application (Ulrich and Hayes, 1997).

A major factor in the complexity of the year 2000 problem is the number of systems that have been effectively an autopilot for perhaps decades. What and how these systems work is entirely unknown to the current users. The fact that the system is somehow interconnected with other systems is very difficult and expensive to figure out (Rao, 1997).

Year 2000 risks vary according to the processing requirements of the organization, whether an organization is privately or publicly held and whether the organization is a government agency. The bottom line is the criticality of computers to the operations of the organization (Ulrich and Hayes, 1997).

Extent

What sounds like a simple computer glitch has enormous ramifications. Most corporations and government entities refuse to talk openly about the year 2000 effect for fear of public embarrassment and mass hysteria. Year 2000 problems are already occurring. According to a technology-consulting firm based in Connecticut , a state correctional facility released several prisoners by mistake due to a computer date data error. The inmates sentence extended well into the next century but the prison's computer system showed they were long over due for release (Simens, 1997).

The year 2000 problem will affect every government agency, business, or individual that uses a computer. Even if an individual does not use a computer, they will still feel the impact. If and when an individual tries to buy insurance, airline tickets, or season passes to sporting events they may encounter trouble. Even automated systems that control a building's heating and cooling systems and ATMs may refuse to work (Celko and Celko, 1997).

This is no minor problem, experts predict that without major adjustments more than 30% of the computer systems in the United States may simply crash and not work at all. Every routine computer transaction or calculation that depend on a date could have problems. Driver's license could be a century expired. The Social Security Administration could think a 25-year-old is 75 or that a 75-year-old is 25. Most new Pentium models use four digit years but 80% of the government and corporations around the world still use older machines. A 1996 congressional survey of top federal agencies found only 9 of 24 had given the Year 2000 any thought. Many agencies with direct responsibilities for providing service to the public such as the Department of Labor, the Veteran's Administration, and the Federal Emergency Management Agency had only minimal Year 2000 initiatives underway (Vistica, 1997).

An electric utility in Honolulu ran test on its' system to see if it would be affected by the Year 2000 bug. The system basically shut down. If the problem had gone unchecked, not only would some customers have lost power but others could have got their power at a higher frequency causing clocks to run faster and other things to burn up. Another concern is with the nuclear power system. The year 2000 problem might affect the security controls and radiation monitoring (Levy and Hafner, 1997).

If no one deals with the Year 2000 problem the phone network would not work properly. Certain commercial operations that run phone systems by computer could also go silent if the software is not fixed. Microprocessors are inside all kinds of devices that have date sensitive controls. The Year 2000 will not make pacemakers stop but it could affect the data read outs it reports to physicians. Some Year 2000 consultants are advising consumers to make hard copies of all their assets. Another possible danger at 12:01 am on January 1, 2000 is air controllers being able to continue tracking planes on radar. A lot of elevators could also malfunction . The elevators, thinking that maintenance is long overdue, will drop to the basement for servicing. Similarly, automobiles having as many as 100 microprocessors that are time challenged may face maintenance defaults. And the sprinkler systems in some buildings may malfunction as a result of faulty embedded systems (Levy and Hafner, 1997).

State governments can find themselves up against a Year 2000 wall. The State of California finished its' inventory last December and found more than half of its' 2,600 computer systems required fixing. Of those, 450 systems are considered mission critical. These are computers that control toll bridges, traffic lights, lottery payments, prisoner releases, welfare checks, tax collection, and the handling of toxic chemicals (Levy and Hefner, 1997).

The problem does not stop with computer programs. Embedded chips are found in everything from the mundane such as VCR's, TV's, elevator systems, motor vehicles, microwave ovens, lawn sprinkler

systems and security systems to the complex devices that help control traffic lights, power generation, water and sewer systems and the control of aircraft. Embedded chips cannot be reprogrammed; they must be replaced. And to replace them, they must be identified and inventoried (Granger and Helms, 1998).

Embedded microprocessors are in consumer electronic devices, kitchen appliances, automobiles, networking equipment, and industrial control systems in one form or another. Though they are usually associated with desktop computers, the most pervasive use of microprocessors is by far in embedded systems. Margolin (1997) describes an embedded system as one that is preprogrammed to perform a dedicated or narrow range of functions as part of a larger system, usually with minimal end-user or operator intervention. With embedded systems gaining network, Web, and Java capabilities, they are getting smarter, more communicative, and more controllable. This can only result in more of them in more applications doing more clever chores (Margolin, 1997).

If the problem is not addressed, a municipality could expect problems in some of its' most critical operations, including traffic signals, fire and police department programs, and court docket systems. And because the problem is only located in computer programs but is hard wired into some circuit boards, it is possible that some crucial equipment such as fire trucks, ambulances, and building controls will be affected by the Year 2000 bug (Granger and Helms, 1998).

Kappelman, Johnson, and Rosemond (1998) found that at a time when the public wants less government, it may be difficult to get some legislatures to step up to the kind of intervention needed. The country would benefit from government assistance in the form of anti-trust exemption so enterprises could freely share their solutions with one another. The government could also allow amortization of expenses incurred as a result of mitigation efforts and letting those companies who want to address the

year 2000 problem get started instead of delaying action and the cost associated with the problem. One beneficial aspect the government could assist with is facilitating the sharing of information on the issue. And the government would do well in certifying some industries as Year 2000 compliant such as nuclear plants, water and sewer systems, oil and chemical pipelines and electrical power generation facilities. Government should assume the responsibility for the public education and monitoring compliance of organizations that provide essential services to the public. These services must be held accountable to be Year 2000 ready. The Federal Communication Commission has been aware of voice telephone system problems that could result in systems failure. The FCC has not initiated any action to ensure local exchanges or the long-distance network is ready for the Year 2000. Kappelman et al. believes state utility commissions should initiate an assessment of all local exchange carriers and long distance providers to see if they are Year 2000 compliant. The assessment should determine if each utility has conducted their Year 2000 risk analysis, developed a corrective action plan and established a date to become Year 2000 ready. The water distribution and treatment systems have smart valves and other microprocessors that control the system. These water utilities should also be asked to analyze their Year 2000 readiness and prepare an action plan. Motor vehicles, highway, and railroad traffic control systems use computer devices with embedded microprocessors that could fail or produce incorrect timing sequences. The Department of Transportation and Railroad Commission should be aware of potential problems and assist local communities with the identification of vendor equipment and systems that may have Year 2000 problems. The DOT and Railroad Commission should work together to assess the safety of highway and railroad crossing sites. And finally, the emergency response community should be aware that the Global Positioning System satellite system may fail in August 1999 due to a date related processing problem. Many of the emergency response systems using GPS to track

emergency vehicles need to be aware of the potential problem and identify vendors offering corrective applications (Kappelamn et al.).

The Year 2000 problem could have an adverse affect on the general public. In Texas, a year 2000 working Group has been established to help government entities and the public address the Year 2000 problem. The department of Information resources and the Texas Association of State Systems for Computing and Communications (TASSCC) have member agencies. According to Mr. Johnson, the fire service is not immune to the Year 2000 problem. Twenty-five percent of all the apparatus made since 1985 have computers or microprocessors on board as an integral part of a maintenance program. Microprocessors that do not recognize the Year 2000 may not allow the truck to start. There is also a concern with the water distribution system, which have smart valves and other automatic computerized controls. Of course, the communications systems rely on computers and are at risk. Mr. Johnson recommends a risk analysis be done for all of these systems and the vendor contacted to establish a Year 2000-readiness plan. A Year 2000-warranty clause should be used when purchasing equipment. Other systems that will concern the emergency response community are the elevator systems, fire alarm systems, traffic control systems and the Global Positioning System. The traffic control systems controlled by computers and the preemption devices used on the traffic signals are dependent on microprocessors that may malfunction. New cars have over forty-seven microprocessors in them. These microprocessors control everything from the heating and cooling of the car to the braking system. Mr. Johnson said, “The type and number of emergencies that may occur as a result of the Year 200 problem can only be estimated at this point but one thing is for sure – the fire service will be in the middle of whatever number that turns out to be.” (Jerry Johnson, Texas Department of Information Resources, phone interview, January 12, 1998).

Overview of technology in the fire service

The fire service has used computer technology in an effort to meet the challenge of the ever changing and demanding environment. An international fire communication network has been organized as a Special Interest Network (SIN). The system will allow a great range of projects and on-line services. The Sin will serve four main functions: communications between fire managers, researchers and educators, publication of documents, maintaining a virtual library and other special services. Other benefits include a rapid dissemination of a world wide information base (Ash, Lord, and Green, 1995).

The computer has changed the way the fire service trains personnel, conducts inspections, develops master plans, and communicates. Computers allow firefighters to train on incidents that are too difficult and dangerous to handle in real life. Users can rehearse an infinite variety of incidents. Virtual reality training can give the novice an experience base, which would otherwise be time intensive and dangerous. Fire inspections have also utilized computer technology. Codes can be assessed on demand and references made to complete a technical inspection. Computers can analyze station location, personnel deployment strategies, cost of services and a host of other issues, which would be almost impossible to analyze otherwise. Using computers to enhance effectiveness is not the only benefit. Fire protection engineers are also taking advantage of the computer to model scenarios that will help them understand fire behavior and allow them to design more effective fire protection systems (Granito, 1995).

The fire officer has many computerized communication opportunities. They include fax machines, electronic file transfer, electronic mail and electronic bulletin boards. Fire safety education can also be

adapted to the computer. Computers allow the fire safety educator to be more creative and reach a special group of young adults who find the computer interesting (Granito, 1995)

Increasing productivity, efficiency, and effectiveness are goals of increased computer use. Computer based emergency service communications has played a major role in the fire service. Computer assisted dispatching has enhanced fire suppression and emergency medical services. Computer assisted dispatching has been a valuable tool in managing the calls for service and resource assignments. Computer interfaces with the communications center CAD system also give the firefighter access to all of the information that the 911 operator has. The responding agency will be able to access cross streets, hydrant information, hazardous materials files, call back numbers, names, and locations on a computer (Hershfield, 1995).

Generally, computerization has been a growing trend in the fire service and the computer software industry has responded by having to meet the needs of this specialized market. Nearly fifty vendors now vie for fire service sales and the number is increasing. The major areas for which the fire service software programs are offered include National Fire Incident Reporting System (NFIRS), personnel scheduling, training, and advancement. Other programs offered are fire prevention records that include pre-fire planning and inspection reporting. For emergency management there are several applications which include emergency medical service reporting, fire apparatus tracking and maintenance recording systems and computer aided dispatching (Wilms, 1991).

From fire department software to enhanced 911 to the FEMA videoconference, computers and satellites have entered the world of fire fighting. The computer and satellite applications are unlimited. In addition to linking several fire fighting agencies together, in the future it will be able to perform tasks such as sending incident videos directly to the incident commander or manager miles away (Robinson, 1987).

Computer software will play a large role in incident management systems. Two recent case histories demonstrate the trend. During Hurricane Hugo and the Loena Prieta earthquake, software played a significant role in the emergency response and area resource management (Christen, 1990).

Some of the programs that are useful to those in fire protection are codes and standards, fire alarm design, and risk analysis. Used properly, these programs can make the job a lot easier. However, if these programs are not used properly then the results can be as dangerous as a fire itself. The most important thing to remember when using fire protection software is that the results of any computer program is no substitute for good, sound judgement (Pucci, 1997).

Computer aided management of emergency operations or CAMEO is also utilized throughout the fire service. CAMEO provides an exhaustive computer database of hazardous materials and chemical properties as well as mapping applications. These applications assist in response, planning, and local operational tasks (Granito, 1995).

Computer programs can simulate fire characteristics and aid in training. Even with years of experience no one can predict with confidence how a fire will burn. A new computer program can help model the fire. The model simulation program uses information about the fuel conditions and the weather to help the firefighter make some predictions on that particular fire. The program, FIRE, can graphically indicate where a fire will move and by when, providing detailed information on the fires' behavior. With that much information, fire managers can devise fire suppression tactics, fire prevention programs, and training sessions in preparation for the fire incident itself (Wagner, 1996).

The Commerce Department's National Institute of Standards and Technology conducts a great deal of fire research, part of which results in software that is useful to the fire service. Fire protection engineers and fire researchers use these NIST programs. Some do have everyday use such as

evaluating new construction, pre-fire planning, public fire education, evaluating fire protection levels and needs and simulating fire fighting methods (Rosenhan, 1993).

Mitigation

There are four methods of dealing with the Year 2000 Crisis:

1.) Do nothing. Wait to see what does not work. This is the choice of a surprising number of small and medium size firms. This alternative may be attractive if the person making this decision is retiring prior to 2000 but the survival of the company is put at risk.

2.) Replace everything. Small firms can afford to replace their software because they do not have large databases. If they chose not to replace their application programs, they can frequently upgrade them by getting the latest software version from the vendor.

3.) Do simple fixes. Many software products offer a simple fix for the existing software. Small changes may be required in the software.

4.) Do a full analysis and complete fix. This involves testing and analyzing systems for potential date problems and making changes to the system. The system must handle a four-digit year and correctly process date data across the centuries (Celko and Celko, 1997).

Muhammad (1997) refers to a five-step process to become year 2000 compliant. The process involves:

1.) Inventory: search throughout the organization for mission critical hardware and software.

2.) Assessment: examine each piece of inventory to find out how the Year 2000 problem will affect it.

3.) Planning and repair: determine how, when and which systems will be upgraded and in what order.

4.) Implementation: complete and install the upgrade.

5.) Testing: uncover any hidden glitches that may have been overlooked.

The organization's systems should now be Year 2000 compliant (Muhammed, 1997).

Companies that are using legacy applications are finding that they do not own and can not get access to the source code. These programs are the older ones that has worked well over the years and no one has paid attention to them until now. It is also very difficult to determine how other software programs interact with the older programs. It is not unusual for a large corporation to have 50,000 modules installed on its' systems. Just analyzing the potential problems there could take years. Many companies will be forced to rewrite applications from scratch and hope they can transfer all of their records to the new system without corrupting the data (Fenton, 1996).

While each industry and organization has a unique Year 2000 challenge, one thing they all will have in common is the legal risk associated with problematic systems. Legal exposures involve potential litigation that may be filed by customers, business partners or other entities because of a system failure or errant data, which caused a financial loss. Other potential incidents involving weapon systems, airplane software, and health care systems could be life threatening. "Because of these many factors, legal considerations are an integral component of the Year 2000 solution. One immediate area that legal teams should focus on is contract management. Any new contracts written for third party software must contain Year 2000 compliance language." (Ulrich and Hayes, p.35) Year 2000 compliance requires that the software and hardware properly handle date dependent information across the century mark. The bottom line on legal issues is that legal counsel must be directly involved in the discussion of the Year 2000 problem (Ulrich and Hayes, 1997).

Insurance companies are offering millennium insurance. Costly business disruptions and lawsuits may occur despite the $300 to $600 billion spent to prepare computers for the year 2000. Those disruptions could cost an additional $1 trillion figuring legal cost and a 5% failure rate. Insurance broker

Marsh and McLennan Inc. is offering an insurance plan in which the likely premium would be up to $5 million for up to $200 million of coverage (Rea, 1997).

What companies have to do is identify the mission critical applications that will affect the organization if they are not converted as well as those things that just simply will not get done and will be left for afterward. Time is not on your side (Vouglas, 1997).

Chief executives know they cannot simply delegate the responsibility for technology to a data person and then move on to other matters. They recognize that the difficult issues such as turf wars, resistance to change, funding, project management and cross-jurisdictional data are issues that the technologist can do little about. These are organizational obstacles that can only be addressed by strong and visible leaders (Cohodas, 1997).

The only sure solution is for the programmers to comb through the millions of lines of programming language in each computer and correct the errant two digit year data. This method is obviously very slow and expensive. Peter de Jager said "If I could change one line of code every second, it would take me the next fourteen years working eight hours a day, five days a week to fix all the lines of code in a small computer system." (Vistica, 1997).

Software companies know that a fortune is to be made with a "bug exterminator." There is no clear leader in the Year 2000 market. However, a California based company by the name of MatriDigm has developed a speedy Year 2000 solution. MatriDigm has spent more than a decade developing the "Code Analyzer". In a trial run the program processed a million lines of code per hour making corrections with about 99% accuracy according to officials (Simons, 1997).

There are Year 2000 companies that have been developed to address the Year 2000 problem. Data Dimensions is on e of those companies and they have developed a program using a proprietary

methodology. The program is called "Template 2000" and is one of the tools used to help companies become Year 2000 compliant (Nocera, 1998).

The City of Tyler's (Texas) Technology Director has been working on getting all of the City departments Year 2000 compliant. If date processing is used in the system, then there is a potential problem. This includes the 911 system, the water distribution system, and vehicles. A risk assessment should be made on all of the systems. Then letters requesting Year 2000 compliance information should be written to the vendor or manufacturer of any suspected problematic system. Information regarding any upgrade should be made also at this time. After systems are upgraded or replaced, they should be tested for compliance. As far as any fire truck or equipment that contain a microprocessor, a legal document should be sent to the manufacturer to confirm that the microprocessor is year 2000 ready (John D'Anna, Technology Director, City of Tyler, Texas, personal interview, January 14, 1998).

PROCEDURES

Project Selection

A project was selected based on the impact an issue may have on both the fire service and the community it serves. As an executive fire officer, it is of paramount importance that the services provided are constantly evaluated and adequate to meet the customer's needs. Also, it is paramount that the future needs of the customer are planned for so that the fire service will be in a position to meet those future needs. The Year 2000 Crisis requires executive support, planning, implementation, and evaluation because the issue has such a potential impact on everything the fire service does in providing

services to the public. A sense of urgency develops as the Year 2000, so often referred to as a distant futuristic date, is now upon us. And it comes at a time when the industrial world has embraced computer technology to such a large extent that technology is now an integral part of our daily lives. Whether the impact is negative or positive, or even transparent, will depend on how we prepare for the Year 2000. It is the challenge of the century!

Research

The Year 2000 Crisis is gaining attention throughout the industrial world. The problem is not new however. Since the early 1990's, there have been numerous articles, books, seminars, and Internet information sites available. The local library and the National Fire Academy's Learning Resource Center were utilized to research periodicals and books. The author also conducted interviews with professionals working on the Year 2000 Crisis. The Internet also has extensive information on the subject and can be found at www.year2000.com. The information that is found on the Internet was helpful and current.

Survey

A survey was formulated by the author and sent 100 fire service colleagues. The survey consisted of 12 questions (Appendix A). The return rate of the surveys sent out was 76 percent. The purpose of the survey was to determine the extent of the use of computer technology in the fire service, the awareness of the Year 2000 Crisis, and what efforts were being made to mitigate the problem. An attempt was made to look at both the internal and external Year 2000 impact. An assessment of the Year 2000 impact on service delivery was made. All surveys were mailed with a stamped self-addressed envelope. There are limitations to the effectiveness of the survey due to the number of survey

mailed, survey content, and return rate. Surveys were mailed back to the author for compilation and analysis.

Assumptions and Limitations

It was assumed all respondents would answer honestly and they would have a basic understanding of the fire service, the service delivery mechanism, the extent technology is used and the Year 2000 Crisis. Factors limiting the survey were the small population surveyed time to develop a more scientific survey and the closed-ended nature of the survey questions.

Definitions

1. Year 2000 Problem: The potential problems and their variation that might be encountered in any level of computer hardware and software from the microcode to application programs, files, and databases that need to correctly interpret year date data represented in two-digit format.
2. Year 2000 Compliant: Information systems and/or applications able to accurately process date data including but not limited to calculating, comparing, and sequencing from, into, and between the twentieth and twenty-first centuries, including leap year calculations.
3. Validation: Testing the results of a year 2000 compliance project at the end of the conversion process to ensure their correctness.
4. System: A set of components that work together within some boundary to accomplish some goal or purpose. Refers to computer based information system consisting of hardware, software, data, procedural, and human components.
5. Testing: The process of executing one or more programs or other component of a system to verify that functional capability of that system meets users' requirements specified during a prior development or maintenance modification.
6. Line of Code: Typically, a single computer program command, declaration, or instruction, although no universal definition exist. Program size is often measured in lines of code.
7. Microcomputer: Personal computer or desktop computer, microcomputer often hosts applications. Originally, the term arose to distinguish these desktop systems from mainframe and microcomputers.

8. Embedded systems: Embedded microprocessors consisting of hardware and software. Embedded systems are found in computers and other electronic devices including those that help control factories, traffic lights, power generators, water and sewer systems, aircraft, automobiles, elevators, fax machines, VCRs, and TVs to name a few.

9. Expansion: In context of the Year 2000 problem, to increase the size of a year data field to accommodate century data, as in expansion from a YY data format to a CCYY format.

10. Inventory: In the context of the Year 2000 project, the process of determining all of the components that comprises the organization's system portfolio. This inventory should include all applications, databases, files, hardware, and other related system components that will require inspection to locate date data and date processing.

11. Application: The general term for both individual compute programs and linked sets of programs that comprise larger entities termed systems.

12. Bugs: Functional and logical errors in software and/or hardware that causes an application to operate a way that is contrary to the way it is suppose to operate.

13. Century date compliant: Status of software that correctly handles any and all activities that use date data without any problems, regardless of century.

14. Contingency plan: A plan for responding to the loss of system or application functionality due to a disaster such as a flood, fire, computer virus, software failure, and /or year 2000 related failures should include considerations of year 2000 related failures of customer and /or supplies.

15. Conversion: The process of making changes to hardware, software, data, and/or procedures in order to achieve century ate compliance.

RESULTS

The Year 2000 Crisis can be defined as the inability of computer technology to correctly process date dependent information across the twentieth and twenty-first centuries. The Year 2000 Crisis is compounded due to the extensive use of computer technology within and outside the organization. The potential problems and their variation may be encountered at any level of computer hardware and software from the microcode to application programs, files, and databases that need to correctly interpret year date data represented in the two-digit format.

The extent of the Year 2000 Crisis can be directly related to the extent to which computer technology is used throughout the world. Computer technology and microprocessors can be found in almost every part of our lives. Even when not working directly with computers, the computer technological advances in the world around them impact people. The Year 2000 Crisis will affect every government agency, business, and individual to some degree. This is no minor problem, Experts predict that without adjustments more than 30 percent of the computers in the United States may fail and 90 percent of the computers worldwide may misinterpret “00”. Every routine computer transaction or calculation that depends on a date could have problems. The problem does not stop with computer programs. Microprocessors or embedded chips are found in almost everything from VCR’s to traffic control systems. An embedded system is preprogrammed to perform a dedicated or narrow range of functions as part of a larger system, usually with minimal end-user involvement. The system can be time sensitive and the year 200 could be misread causing a malfunction.

The fire service utilizes computer technology in all areas of service. As the survey indicates, computers can be found in the administrative, training, maintenance, and prevention divisions. The suppression and emergency medical divisions also utilize computer technology to enhance services. Computer technology has allowed a higher level of efficiency and effectiveness. A large amount of data can be processed and records maintained over a wide range of experience. As fire departments upgrade in an effort to increase the level of service, a greater dependency on computer technology will develop. In addition to that, the interaction with an external environment will also increase the level of involvement with computer technology.

Mitigation efforts for the Year 2000 Crisis will not be unlike those efforts used to address other impending emergencies. There is a need to assess the risk, the impact, mitigation efforts, and contingency plans. This is assuming one has chosen to respond to the problem at all. Waiting to see what will happen is an alternative. However, an effective, proactive fire officer will see the value of executive planning here. Once a decision is made to respond to the Year 2000 Crisis, a five-step process can help bring the organization to Year 2000 compliance. That process is:

1. Inventory: search the organization for mission critical hardware and software.
2. Assessment: examine each piece of inventory to assess the Year 2000 problem impact.
3. Contact vendor or manufacturer for Year 2000 compliance and upgrade information. Plan and repair: determine how, when and which system will be upgraded and in what order.
4. Implementation: complete and install upgrade.
5. Testing: uncover any hidden glitches that may have been overlooked.

Instrumentation

An analysis of the survey sent to 100 fire service colleagues follows. Seventy-six percent of the surveys were returned to the author. The respondents answered the survey in the following manner:

1.) In what ways are computers used in your department?

Administration 99%

Maintenance 82%

Dispatch 78%

Purchasing 72%

Training 84%

Research 51%

Inspection 78%

Other – planning, hazardous materials, finance, ambulance reporting, Internet, run reports, networking, inventory, mapping, personnel, investigation, payroll, public education.

2.) Does any of the department software programs contain date dependent data?

Administration 78%

Communication 47%

Statistical Records 77%

Personnel Reports 58%

Security Alarms 16%

Dispatch 65%

Inspection 59%

Payroll 61%

Inventory 43%

Training 65%

Purchasing 46%

E-Mail 39%

Maintenance 50%

3.) What kind/type of equipment in the department may have embedded computer microprocessors?

Fax Machines 77%

Alarm Systems 27%

Vehicles 51%

Heat/AC 35%

Don't Know 20%

Other – phones, defibrillators, gas detectors, portable radios, bar coding, thermal detector, chemical detector.

4.) Does your department utilize the services of a Chief Information Officer/Technology Director to address technology issues?

Yes 47%

No 53%

5.) Do you require all technology acquisitions to be Year 2000 compliant?

Yes 57%

No 15%

Don’t Know 28%

6.) Is your department engaged in any Year 2000 compliance programs?

Yes 46%

No 34%

Don’t Know 20%

7.) Has your department experienced any problems related to the Year 2000 compliance issue related to date dependent data?

Yes 9%

No 68%

Don’t Know 23%

8.) Have funds been appropriated in your department to address the Year 2000 compliance issue?

Yes 24%

No 61%

Don’t Know 15%

9.) Is the 911 system Year 2000 compliant?

Yes 36%

No 9%

Don’t Know 54%

10.) Is the dispatching in your department Year 2000 compliant?

Yes 46%

No 14%

Don’t Know 40%

11.) Is the communications equipment in your department year 2000 compliant?

Yes	47%
No	9%
Don't Know	44%

12.) Is the water distribution system in your area controlled by computers or microprocessors?

Yes	31%
No	18%
Don't Know	51%

If yes, is it Year 2000 compliant?

Yes	7%
No	1%
Don't Know	24%

DISCUSSION

The Year 2000 Crisis has been defined as the inability of computer technology to recognize the new millennium – the year 2000. This historical event has a special meaning and impact due to the embrace the world has of technology. Outside of the issue of being beneficial, the extent to which computer technology has become part of our lives is so pervasive it is hard to imagine a day or action that is not touched by it.

To the extent that the year 2000 will actually clash with the technological world is yet to be determined. However, documentation exist which supports a believable chance of widespread repercussions if the issue is not taken seriously.

Each organization will have their own concerns and mitigation efforts. No one organization will be immune and the impact that the Year 2000 Crisis will have will be dependent on the executive planning made to address the issue.

The results of the author's survey reveal an extensive use of computer technology in the fire service. The administration, training, maintenance, prevention, emergency medical, and suppression activities of the fire service are all impacted by computer technology. In some cases, this is to the extent that it is transparent and our dependency on technological assistance has become addictive. As critical as computer technology is to the fire service, almost fifty percent of the departments surveyed do not utilize the services of a Chief Information Officer or Technology Director.

Approximately half of the departments surveyed do recognize the Year 2000 Crisis and require acquisitions to be Year 2000 compliant. However, there appears to be a lot of work to be done prior to 2000. The systems in the organization that are using computer technology require a careful risk

assessment and analyzed as a component in the service delivery mechanism. From communications to hydraulics, from fax to incident command, we depend on computer technology to get it done. A sense of urgency should become evident as the Year 2000 Crisis unfolds in your own backyard causing everything from minor inconveniences to serious life safety problems. It is imperative that the fire service plan and prepare for the year 2000 – to do otherwise would be reckless. As the year 2000 materializes over the next twenty-one months, the fire service should prepare itself and be in a position to continue to operate and respond to emergencies. Anything less will be unacceptable!

RECOMMENDATIONS

It is recommended that every fire service member start to work on the Year 2000 Crisis. The effort begins with the fire executive and must be supported throughout the project until completion. As each day passes, the year 2000 draws closer, and whether the fire service is ready or not, the year "00" will arrive. The pervasiveness of computer technology has filled at least a small part of every aspect of our lives. That pervasiveness must be analyzed and understood. Will the computer technology that has driven us beyond the possible now make everything impossible?

It is recommended that each organization apply a five-step mitigation process to address the Year 2000 Crisis – Inventory, Assessment, Planning and Repair, Implementation, and Testing. In the planning phase, it is important to contact vendors and manufacturers for Year 2000 compliance and upgrade information. This process should be applied to all systems within the organization. Also, a careful analysis should be made of external factors that may impact the fire service i.e. alarm systems, traffic

control systems, and water distribution systems to name a few. The environment in which the fire service operates may be in for a drastic adjustment at the dawning of the new millennium. Therefore, careful planning and preparation must be done. Contingency planning must also be a part of the mitigation efforts.

There has never been another time in our history that the fire service has been faced with such an enormous, pervasive, worldwide problem. But the world won't solve the problem. The fire service must be prepared and not become a part of the crisis. The alarm has been sounded. We know what the problem is, how the problem developed, and why. Now respond! It may be the most crucial emergency management effort of the twentieth century – to mitigate the impact of the Year 2000 Crisis and the twenty-first century.

REFERENCE LIST

Celko, J., & Celko, J. (1997). Double zero. Byte,22,(7), 89-94.

Chaabouni, M. (1998). A framework for testing year 2000 application conversions. [On-Line]. Available: http://www.year2000.com/archive/chaabouni.html.

Christen, H. (1990). Software and incident management. Firehouse,August, 82.

Cohodas, M. (1997). Bridging the geek gap. Governing,10(2), 72.

Fenton, B. (1996). The microprocessor turns 25. Popular Mechanics,173,(11), 30-32.

Granger, D., & Helms, M. (1998). Year 2000: a legal odessey into the new millennium. Unpublished manuscript, Law firm of Akin, Gump, Strauss, Hauer, & Feld, Austin, Texas.

Granito, J. (1995). From hoselines to online. NFPA Journal, Jan./Feb., 77-83.

Herschfield, V. (1995), How colorado springs uses computer mapping. NFPA Journal, Jan./Feb., 84-86.

Kapplemann, L., Johnson, J., & Rosmond, K. (1998). The role of government in solving the year 2000 computer problem. [On-Line]. Available: http://www.year2000.com/archive/government.html.

Levy, S., & Hafner, K. (1997). The day the world shuts down. Newsweek,129,(22), 53-59.

Margolin, B. (1997). Smarter stuff. Byte,22,(6), 85-92.

Muhammad, T. (1997). The 2000 year glitch. Black Enterprise,27,(10), 38-40.

Nocera, J. (1996). The story of "00". Fortune,134,(4), 51-62.

Pucci, W. (1997). Hot software for the fire protection community. NFPA Journal, Jan./Feb., 51-56.

Rao, R. (1997). How serious is the year 2000 problem? [On-Line]. Available: http://www.year2000.com/pub/year2000/y2kfaq.txt.

Rea, A. (1997). Does your computer need millenium coverage? Business Week, March 10, 98.

Robinson, R. (1987). USFS computer puts the byte on wildland fires. American Fire Journal, June, 22.

Rosenhan, A. (1993). The pyro pc. Fire Chief, Dec., 24-26.

Simonelli, M. (1997). Financial complications aggravate year 2000 glitch. Contingency Planning & Management,11,(4), 1-5.

Simons, J. (1997). The millennium looms. U.S. News & World Report,Feb.17, 54.

Ulrich, W., & Hayes, I. (1997). The year 2000 software crisis. New Jersey: Prentice Hall PTR.

Vistica, G. (1997). I'm sorry, sir, but the 20th century just disappeared. Newsweek,124,(4), 18.

Vouglas, B. (1997). Year 2000 computer timebomb's ticking away. Contingency Planning & Management,2,(6), 28.

Wagner, M. (1996). Fighting fire with fire. National Fire & Rescue,20,(2), 57-60.

Wilms, P. (1991). Surveying today's fire service software. NFPA Journal, May/June, 91-103.

APPENDIX A

Year 2000 Crisis Survey

1. In what ways are computers used in your department?

   Administrative __

   Maintenance __

   Dispatch __

   Purchasing __

   Training __

   Research __

   Inspection __

   Other __

2. Does any of the department software programs contain date dependent data?

   Administration __

   Communication __

   Statistical Records __

   Personnel Records __

   Security/Alarm Systems __

   Dispatch __

   Inspection __

   Payroll __

   Inventory __

   Training __

Purchasing __

E-Mail __

Maintenance __

Other __

3. What kind/type of equipment in the department may have embedded computer microprocessors?

   Fax Machine __

   Alarm Systems __

   Vehicles __

   Heat/AC Systems __

   Other __

   Don't Know __

4. Does your department utilize the services of a Chief Information Officer/ Technology Director to address technology issues?

   Yes __

   No __

5. Do you require all technology acquisitions to be year 2000 compliant?

   Yes __

   No __

   Don't Know __

6. Is your department engaged in any year 2000 compliance program?

   Yes __

   No __

Don’t Know __

7. Has your department experienced any problems related to the year 2000 compliance issue related to date dependent data?

   Yes __

   No __

   Don’t Know __

8. Have funds been appropriated in your department to address the year 2000 compliance issue?

   Yes __

   No __

   Don’t Know __

9. Is the 911 System year 2000 compliant?

   Yes __

   No __

   Don’t Know __

10. Is the dispatching ion your department year 2000 Compliant?

    Yes __

    No __

    Don’t Know __

11. Is the communication equipment in your department year 2000 compliant?

    Yes __

    No __

    Don’t Know __

12. Is the water distribution system in your area controlled by computers or microprocessors?

    Yes __

    No __

    Don't Know __

    If yes, is it year 2000 compliant?

    Yes __

    No __

    Don't Know __